Strategy Research Project

Enabling Combatant Commander's Ability to Conduct Operations in the Cyber Domain

by

Colonel Charles N. Eassa
United States Army

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
03-03-2012	Strategy Research Project	

4. TITLE AND SUBTITLE
Enabling Combatant Commander's Ability to Conduct Operations in the Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Charles Eassa

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Dr. Jeffrey L. Groh
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Combatant commanders are the focal point of joint operations to apply military power in pursuit of national security objectives. They execute "operations characterized by a complex, interconnected, and global operational environment." No arena highlights this challenge more than the Cyber Domain. The Department of Defense has exerted tremendous resources to meet the challenges in this dynamic domain. Despite these efforts, combatant commanders lack the ability, agility, and common understanding to execute their assigned missions and responsibilities now and for the immediate future in the cyberspace domain. This paper will exam the combatant commander's role in operations framed by joint doctrine with an emphasis on the *Joint Operational Access Concept*. This concept sets up criticality of the cyber domain, the necessity to develop cross-domain synergy, and highlights the combatant commander's responsibility. Then the paper examines emerging cyber doctrine and concepts. This enables a comparison of current joint doctrine, cross-domain synergy, and emerging cyber doctrines and concepts. The paper highlights shortfalls and provides recommendations that can improve both doctrine and operations.
.

15. SUBJECT TERMS
Cyberspace, Cyber Domain, Command and Control

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	26	

USAWC STRATEGY RESEARCH PROJECT

ENABLING COMBATANT COMMANDER'S ABILITY TO CONDUCT OPERATIONS IN THE CYBER DOMAIN

by

Colonel Charles N. Eassa
United States Army

Dr. Jeffrey L. Groh
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Charles N. Eassa

TITLE: Enabling Combatant Commander's Ability to Conduct Operations in the Cyber Domain

FORMAT: Strategy Research Project

DATE: 3 Mar 2012 WORD: 5,131 PAGES: 26

KEY TERMS: Cyberspace, Cyber Superiority, Cyber Warfare, Cyber Operations

CLASSIFICATION: Unclassified

Combatant commanders are the focal point of joint operations to apply military power in pursuit of national security objectives. They execute "operations characterized by a complex, interconnected, and global operational environment."[1] No arena highlights this challenge more than the Cyber Domain. The Department of Defense has exerted tremendous resources to meet the challenges in this dynamic domain. Despite these efforts, combatant commanders lack the ability, agility, and common understanding to execute their assigned missions and responsibilities now and for the immediate future in the cyberspace domain. This paper will exam the combatant commander's role in operations framed by joint doctrine with an emphasis on the *Joint Operational Access Concept*. This concept sets up criticality of the cyber domain, the necessity to develop cross-domain synergy, and highlights the combatant commander's responsibility. Then the paper examines emerging cyber doctrine and concepts. This enables a comparison of current joint doctrine, cross-domain synergy, and emerging cyber doctrines and concepts. The paper highlights shortfalls and provides recommendations that can improve both doctrine and operations.

ENABLING COMBATANT COMMANDER'S ABILITY TO CONDUCT OPERATIONS IN THE CYBER DOMAIN

> We are living in an age where the right information, at the right time, drives greater mission effectiveness.
>
> —Michael J. Basla[2]

Given the breadth of the United States *National Military Strategy* and the focus on defending the homeland forward, Joint Publication 1 *Doctrine for the Armed Forces of the United States* states that Combatant Commanders (CCDRS) are the focal point for application of military power. They execute "operations characterized by a complex, interconnected, and global operational environment"[3] while coordinating with supporting CCDRs on required capabilities. With limited or declining resources, increasing requirements, and an evolving security atmosphere, their aptitude to meet these new conditions is essential to the security of the United States and its interests. No arena highlights this challenge more than the Cyber Domain. President Obama called attention to the importance of" an open, interoperable, secure, and reliable cyberspace" with the publication of the "International Strategy to Secure Cyberspace" in May 2011. Previously, the Department of Defense (DOD) designated cyberspace a global domain within the information environment, elevated its status to a warfighing domain in 2009, and published the *DOD Strategy for Operating in Cyberspace* in July 2011. The U.S. government has since released a series of polices, initiated numerous interagency processes, and embarked on multiple actions to shape the Nation's approach to this exigent and evolving national security challenge. Despite these efforts, combatant commanders lack the ability, agility, and common understanding to execute their assigned missions and responsibilities now and for the immediate future in the

cyberspace domain. Framing a combatant commander's ability, agility, and common understanding in executing major contingency operations and comparing these against the emerging doctrine of the Cyber Domain will highlight shortfalls and provide recommendations that can improve both doctrine and operations.

Joint operations are the hallmark of how the United States brings the military instrument to bear across the range of military operations. To accomplish this, CCDRs must integrate the cyber domain seamlessly with the other warfighting domains to provide the Nation options. This action enables freedom of action and the understanding to effect the operational environment through use of rapidly changing technology. This paper uses emerging joint doctrine and concepts to highlight the differing perspectives. Using the foundations laid out in current joint doctrine, the paper examines how cyber operations doctrine strengthens, detracts, or confuses how a geographical combatant commander (GCC) commands and controls major military operations in his or her area of responsibility. The primary effort to accomplish this will focus on review of joint doctrine and an examination of emerging cyber doctrine. The paper will identify shortfalls and develop recommendations to assist the joint community in resolving and adding clarity to this critical endeavor facing the nation and its national security for the twenty-first century.

National Strategic Guidance

The President's guidance for the role of cyberspace at the national level delineates multiple means to frame CCDRs' approaches. The subtitle to the President's *International Strategy for Cyberspace*; *Prosperity, Security, and Openness in a Networked World* highlights the opportunities, tensions, and challenges that accompany this evolving arena. As cyberspace remains an anarchical field[4], the President is

cautious and conscious not to develop an overbearing military approach that could impede the diplomatic and economic effects cyberspace brings.[5] The *National Security Strategy* of May 2010 amplifies the tensions listing the imperative to advance U.S. interests contrasted against the statement that the nation's "Armed Forces will always be a cornerstone of our security but they must be complemented."[6] The *National Security Strategy* highlights the dependency of the nation on cyberspace, the vulnerability to attack, and disruption posed to the United States. This is recognition that cyberspace transcends traditional approaches to national security.

This recognition has yet to emerge into a unified vision and approach to national security. Unlike the historical precedent set by the unifying threat of nuclear weapons, each cabinet member acknowledges the challenges and opportunities but sees the cyber domain differently. The Department of Homeland Security (DHS) is the lead agency to secure cyberspace.[7] The Government Accounting Office found that DHS has not fully satisfied its responsibilities designated by the national cybersecurity strategy.[8] Combatant Commanders struggle under current doctrine to achieve their number one purpose of defending the homeland in this evolving and dynamic environment. While not the focus of this paper, the processes, procedures, and common understanding in cyberspace lack the definition and clarity similar of other interagency efforts like arms control, counterterrorism, and security force assistance. The President and Secretary of Defense reinforce this in their vision as articulated in *Sustaining U.S. Global Leadership; Priorities for 21st Century*.[9]

Military Direction

The *National Military Strategy* designates the core tasks of defending the Nation and winning its wars to the Department of Defense.[10] Again, joint doctrine states that the CCDRs are the focal point of this effort. Unlike the clarity provided by years of experience in other aspects of national security, it states, "we must seek executive and Congressional action to provide new authorities to enable effective action in cyberspace".[11] To a combatant commander, this highlights the ambiguity of his role and responsibilities in cyberspace. The interagency will solve this issue in time. However, this does not assist in developing, resourcing, or planning for the future demanded by budgets, theater campaign plans, contingency planning or crisis planning. Compounding this is the reduction of resources and personnel driven by budget demands, shifting of focus to the Pacific, and the new policy of having a smaller, technologically superior force that is increasingly dependent upon cyberspace. For the immediate future, combatant commanders must assess their responsibilities without experience and the benefit of a comprehensive, resourced, and unified national approach.

The best framework to exam these dynamic changes is the *Joint Operational Access Concept* (JOAC).[12] This concept summarizes the enduring requirement for force projection, the concepts of antiaccess and area-denial[13], and the importance of preconditions cast against three trends:

(1) The dramatic improvement and proliferation of weapons and other technologies capable of denying access to or freedom of action within an operational area.

(2) The changing U.S. overseas defense posture.

(3) The emergence of space and cyberspace as increasingly important and contested domains.

The JOAC highlights the changing operating environment and austere environment facing the Nation.

To combatant commanders, the JOAC has a central thesis of cross-domain synergy that is central to their requirement to integrate all aspects of military power. Cross-domain synergy is defined as the "complementary vice additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others".[14] This enables the establishment of superiority in some combination of domains that provides the freedom of action required by the mission.[15] As CCDRs can no longer afford to assume the movement of capabilities into an area of operation (AO) will be uncontested and that the ability to operate within the AO freely, this emphasizes the critical requirement of cyberspace as a warfighting domain and one that underpins the other domains.[16] The JOAC coins this as operational access that is “the ability to project military force into an operational area with sufficient freedom of action to accomplish the mission.”[17]

Combatant commanders must account for the evolution of cyberspace within the Department of Defense to gain perspective. Five years ago, cyber was widely recognized as an enabling function. Given its increasing importance and lessons learned from global operations, the Department of Defense designated cyber a fifth warfighting domain in 2009. Corresponding to enable capability and capacity, the Department of Defense established U.S. Cyber Command (CYBERCOM) as a

subunified command under U.S. Strategic Command. Since these inceptions, each Service has embarked on identifying the cyberspace impacts on their approach to military operations within their domain. While this affects their organization, structure, and personnel, it also influences their contribution to joint doctrine and CCDRs' efforts. The U.S. Navy has created an Information Dominance Corps[18] and the U.S. Air Force has created cyberspace operations officers.[19] The signal and intelligence communities within the Navy and Air Force have primarily conducted these efforts. This brings a nuanced technological approach rather than an operational methodology as laid out in Joint Publication 3 *Joint Operations*. The Services are working to overcome the central challenge of describing the art of warfighting and operating in this new domain. Understanding this enables CCDRs to integrate these capabilities and gain the cross-domain synergy. The Department of Defense's efforts and organization complicates this endeavor because of decentralization across various offices, commands, services, and military agencies.[20] Combatant commanders bear the burden to achieve national objectives under the duress of an operational crisis in an opaque cyberspace environment.

As the Department of Defense uses capabilities-based planning, CCDRs play an increasingly prominent role in identifying and prioritizing potential adversarial threats, required countermeasures, and required capabilities for amalgamation to achieve national objectives.[21] Joint Publication 1 *Doctrine for the Armed Forces of the United States* recognizes that operations conducted by CCDRs will focus on the threat "across geographical regions that include forward regions, approaches, the homeland, and in cyberspace."[22] It continues, "The divisions among the geographical regions are not

absolute and may overlap or shift depending on the situation and threat."[23] This challenges the principle of joint operations to maintain unity of command of all capabilities, command, and control under one commander.[24] Joint doctrine expands on this by stating functional combatant commanders support geographic combatant commanders. As geographical combatant commanders remain the focus given their area of responsibility (AOR), there is considerable tension as functional combatant commanders seek to command and control their capabilities operating in a GCC despite operating only in a specific domain and in a limited range of military operations. [25] Department of Defense can only resource the five warfighting domains at geographical combatant commands under current doctrine and constraints.[26]

Geographical combatant commanders remain the crucial connection between "national security policy and strategy and the military forces that conduct military operations within their geographical AORs" to facilitate "effective coordination of the operations within that area."[27] Their ability to integrate joint forces and capability to generate cross-domain synergy is imperative. The advantage of this approach is that it extends beyond the immediate operational environment and across the range of military operations. Geographical combatant commanders have the resources, authority and responsibility across the range of military operations to "tailor forces for the mission at hand, selecting those that most effectively and efficiently ensure success."[28] They must constantly balance their theater campaign plan, high probability missions, and Joint Strategic Capabilities Plan assigned missions against their resources to generate cross-domain synergy at the time and place of their choosing to accomplish desired national objectives.

To assist CCDRs in developing this cross-domain synergy with capabilities that may not reside in the geographic combatant commanders' arsenal and by doctrine, the Joint Chiefs of Staff designates the supporting CCDRs. While this designation may take many forms by doctrine, the designated supported combatant commander must identify both the capabilities and relationship required to accomplish the assigned mission. Accomplished normally during the planning phase, the supported commander determines the specifics of the support relationship. Ascertained in coordination with the supporting command, the details describe the purpose of the support relationship, the effect desired, and the scope of the action to be taken. Essential elements of this include:

(1) The time, place, level, and duration of the supporting effort.

(2) Relative priority of the supporting effort.

(3) Authority, if any, of the supporting CDRs to modify the supporting effort in the event of exceptional opportunity or an emergency.

(4) Degree of authority granted to the supported CDR over the supporting effort.

(5) Establishment of air, sea, and ground maneuver control measures and cyberspace operations protocols.

(6) Development of target nominations, establishment of fire support coordination measures and the role of coordination centers.

(7) Development of the intelligence collection plan.

(8) Force protection responsibilities.[29]

This framework empowers a common dialogue and understanding that is mission specific. It reinforces that joint doctrine is commander centric and retains unity of

command.[30] The supporting commander "determines the forces, tactics, methods, procedures, and communications to be employed in providing this support" and ensures support requirements are communicated."[31] This enables their actions to be consistent with the supported commander's strategy. It allows them to tailor their tasks, forces, and resources, establish operational limitations such as rules of engagement (ROE), constraints, and restraints. The supporting CCDRs develop these concepts of operations (CONOPS) into OPLANs and operation orders (OPORDs) that enables the supported CCDRs' cross-domain synergy.[32]

The supported CCDR often will have a role in accomplishing more than one national strategic objective during a joint operation. Some of these national objectives necessitate use of other national instruments of power. The combatant commander must coordinate through appropriate doctrinal mechanisms to enable attaining the necessary resources. As laid out in the JOAC, the CCDR must accept that a contested cyberspace is part of the operating environment. The CCDR's ability to understand and set preconditions demand a whole of government approach as authorities and capabilities reside with other agencies. This collaboration requires a unity of effort and commonality of understanding that current does not exist. Like cross-domain synergy, this collaboration enables the greater opportunity while limiting vulnerabilities. Establishing an air bridge to provide uninterrupted logistics provides an example of this cross-domain synergy. Challenged by different perspectives, demands, and resource levels, all other agencies are working through the impact of the cyber domain on their own endeavors. While this issue is beyond the scope of this paper, it is imperative to

resolve quickly. Current Joint Interagency Coordination Elements at combatant commands lack proper expertise focused on the cyber domain.

Framing the Cyber Domain

Joint doctrine does not define the relationship between the cyber domain and the other domains. It defines the cyber domain as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[33] The operational environment enables CCDRs to understand their "conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[34] This framework facilitates the development of cross-domain synergy by understanding the complexity, interconnectivity, and relationships. Combatant commanders must approach their operational environments to gain a broad understanding of the obstacles, time constraints, and effort required to accomplish their purpose. Understanding the operational environment allows greater cross-domain synergy while identifying vulnerabilities and opportunities. Disaggregating the operational environment, the *Joint Concept for Operating in Cyberspace* states cyberspace comprises of a physical layer, a logical layer, and a social layer.[35] This challenges CCDRs as current doctrine does not lay out this construct for any other domain nor does the relationship of these layers correspond to the operational environment.

Traditionally, CCDRs frame their operational environment by geography. The cyber domain transcends this but given current doctrine and limited ability to visualize the cyber domain against the other domains, this technique remains valid. Further

framing can employ areas of interest, areas of influence, and systems approaches. This empowers CCDRs and permits for cyber domain influences and desired effects that traverse traditional boundaries. Given today's limited capability, CCDRs are constrained in their ability to see the operational environment through the cyber domain to develop cross-domain synergy.

Joint doctrine provides a standard approach for describing the cyber domain by using operational art. Operational art is:

> A thought process that uses skill, knowledge, experience, and judgment to overcome the ambiguity and uncertainty of a complex environment and understand the problem at hand. Operational art also promotes unified action by encouraging JFCs and staffs to consider the capabilities, actions, goals, priorities, and operating processes of interorganizational partners, while determining objectives, establishing priorities, and assigning tasks to subordinate forces. It facilitates the coordination, synchronization, and, where appropriate, integration of military operations with those of interorganizational partners, thereby promoting unity of effort.[36]

Using this approach and the six basic joint functions listed in Joint Publications 3-0, *Joint Operations*, enables CCDRs to frame the cyber domain. The joint functions (C2, intelligence, fires, movement and maneuver, protection, and sustainment) provide the foundation "common to all joint operations."[37] This expands on current cyber and emerging doctrine that describe cyber domain activities as defensive computer operations, net operations, and offensive computer operations. Combatant commanders can use this framework to visualize the adversarial, friendly, and neutral systems and functions, their interaction, and assess their relation to the operating environment. It enables greater collaboration with supporting combatant commanders, interagency participants, and other external actors to highlight cross-domain synergy.

Towards Common Understanding

To achieve capability and agility, the CCDR must have a staff composed of those who understand adversaries, their capabilities, understand the operating environment, and can direct assigned forces or capabilities to accomplish the assigned mission.[38] The CCDR must then match each service component to its capabilities to accomplish their assigned missions within their capabilities.[39] As joint doctrine highlights, commanders are the central point in developing operational art due to their experience and judgment. "Commanders draw on operational art to mitigate the challenges of complexity and uncertainty" to leverage "their knowledge, experience, judgment, and intuition to generate a clearer understanding of the conditions needed to focus effort and achieve success."[40] Commanders must visualize, describe, direct and constantly assess their actions to achieve their purpose. Staffs organize along functional lines to provide relevant information for the CCDR to make decisions.

The CCDR and the staff work together to determine what success is during the planning phase and seeks approval from the assigning headquarters. Success is generally measure in positive terms of accomplishing the desired national objective. Rarely is the national objective or endstate focused on one aspect of operating spectrum or warfighting domain. The CCDR and staff focus on creating cross-domain synergy to leverage advantages and minimize the risks across the operational environment.[41] This entails a dialogue with component commanders, supporting combatant commanders, and other influencer that affect the cyber domain. This dialogue must translate the desired national objectives into effects and tasks that each actor can understand.

As articulated in the JOAC, combatant commanders starting this dialogue depend on setting preconditions required to overcome area denial and antiaccess challenges – potential or real. These preconditions require actions, effort, and activities be conducted with ample time to frame the operational environment for the supported CCDR. This requires an unprecedented level of agility and collaboration. This agility must account for each combatant commander's mission, the different means available, and the operational tempo. To define agility, the supported commander must be able to understand the changes in the operating environment by external influences and those of the adversary and be able to make decisions that shift capability and refine efforts to accomplish the mission. Given the pace of actions in the cyber domain and the definition of success, the CCDR's upfront dialogue sets in motion collaboration at multiple levels.

Central to creating this condition of agility is common understanding. Given the complexity and nascent experience in relation to warfighting in the cyber domain, both the supported and supporting combatant commanders must use existing joint doctrine to build trust and confidence to achieve common understanding. While each may have a different perspective, the JOAC provides a framework to lay out details to establish the operational approach.[42] Employing operational design extends operational art's vision with a creative process that helps answer the ends–ways–means–risk questions and builds common understanding. This common understanding of this complex and dynamic environment enable both the supported and supporting commanders to communicate more effectively, understand the relationships and dependencies between each other's activities, and thus, create greater synergy.

Examination of Emerging Cyber Operations Doctrine

Cyber doctrine is emerging but the Joint Staff published a *Joint Concept for Cyberspace* (JCC) in October 2011.[43] As joint doctrine codifies current practices and their integration that enables cross-domain synergy, the challenge of designating cyber as a warfighting domain did not emerge from a common understanding or universal practices. Combatant commanders bear the burden and must work through the perspectives provided by the various actors.

The *Joint Concept for Cyberspace* uses the *Joint Operating Environment*[44] to frame the challenges but does not use the concepts laid out in the JOAC. The JCC's uses an ends-ways-means approach. The end is listed as cyberspace superiority. The ways to achieve this are DoD Global Information Grid Operations (GIG Ops), Offensive Cyberspace Operations (OCO), and Defensive Cyberspace Operations (DCO).[45] The means are a mixture of warfighting functions, joint precepts, and enterprise management processes. This ends-means-ways approach does not correspond well with developing cross-domain synergy as CCDRs will primarily use national security objectives as the ends. Combatant commanders seek to establish conditions like cyberspace superiority to enable other actions and activities that accomplish desired objectives. Cyberspace as an end does not accomplish objectives but it is a starting point for cross-domain synergy.

The concept of cyber superiority mirrors air and maritime superiority. The challenge is that air and maritime superiority have a tangible physically measurable property where as the cyber domain remains unbounded. The framework of offensive cyber operations, defensive cyber operations, and network operations does not

adequately support this concept. Network operations essentially are an enabling function and while critical, are subordinate to offense and defense. There is merit to designating an entire operation with the purpose of maintaining this enabling function globally and having each combatant command write a corresponding supporting plan.[46] The activities must support objectives in cyberspace as well as the other domains. The CCDR must understand the operational dependencies, vulnerabilities, and emerging opportunities that enable cyber superiority and cross-domain synergy. This cross-domain synergy must achieve cyber superiority.[47] To gain superiority, the CCDR must have unfettered access in a constantly evolving and always contested environment. This requires a greater degree of integration of actions and capabilities and at lower echelons than ever before to achieve this effect.[48] Actions at all levels focus on ensuring required information flows through the cyber domain while maintaining access or control of the infrastructure necessary to gain cyber superiority.[49] While this is adversarial focused and applies in terms of anti-access and area denial,[50] it may be a limiting construct beyond as it does not account for the complexity and reach of all the potential actors in cyber.

Achieving superiority focuses on employing capabilities in a sequence to accomplish tasks that achieve desired effects. While Joint Publication 5-0, *Joint Operational Planning*, uses operational art and design to express this, emerging cyber doctrine focuses on the technology and information assurance aspects than on the art and experience of warfighting in cyberspace. The JOAC requires enduring requirement for force projection and demands recognition of cyberspace as increasingly important and contested domain. The cyber domain must focus on use language that enables

CCDRs an understanding and the ability integrate the requirement of cyberspace superiority as a cross-domain synergy.

Equally important is what the emerging doctrine and concept does not articulate. The first is the scope of cyber operations. Cyber operations may be as extensive as a global campaign[51] to enable global force projection and national security objectives and as small as an enabling function on a show of force. Scope drives resources and operational tempo. The operational tempo and decisions in the cyber domain are different from the operational tempo and battle rhythm of other domains because cyber effects can have impact in nanoseconds globally. Without this discussion, the cyber domain remains unbounded and unframed for CCDRs. This affects discussions on service responsibilities that combatant command components must accomplish is support of their forces and missions. The second is the nature that combatant commands are dependent on force projection capabilities that will require support from interagency and combatant commanders. As an example, securing the command and control of forces flowing from CONUS to a CCDR's Joint Staging Area requires a detailed supporting plan. This supporting plan requires actions, activities, and resources to set the preconditions for operations. The third is that the correlation between the joint functions as outlined in Joint Publication 3-0, *Joint Operations*,[52] and the broad mission areas of cyberspace operations (GIG Ops, DCO, OCO) falls on combatant commanders to extrapolate to gain agility. The joint functions “reinforce and complement one another” and seek to develop synergy across the functions as "essential to mission accomplishment”[53]. As an enabling function, GIG Ops creates cross-domain synergy and underpins all joint functions. As broad operations descriptions, OCO and DCO work

across all the joint functions in some combination to maintain a desired level of cyber superiority. Just as all operations contain aspects of offense, defense, stability, and support, the mission areas of the cyber domain do not afford clarity.

Recommendations

A More Comprehensive Approach. As the JOAC lays out new challenges, CCDRs require a better framework for describing activities in cyberspace to afford greater cross-domain synergy than GIG OPS, DCO, and OCO. U.S. European Command used the following missions to provide clarity and enables greater collaboration across the domains:[54]

(1) Counter Cyber – Ability to protect networks.

(2) Power Projection – Ability to achieve effects in and through cyber domain.

(3) Command and Control – Ability to direct, coordinate, report, and assess efforts.

(4) Intelligence, Surveillance, and Reconnaissance – The ability to gain and maintain situational awareness as well as conduct target and system development.

(5) Transactions – The business applications of the cyber domain that occur millions of time a day but may provide opportunities and vulnerabilities to the operation.

(6) Relations – Ability to understand the social network, relationships, and influences on the assigned mission.

The advantage is greater task focus on mission accomplish and less requirement on the part of the other domains to comprehend how the cyber domain integrates into their

operations and effects. The disadvantage is this would expand the complexity and development timeline of detailing and integrating these tasks. This delay will cause a short-term operational risk as most cyber requirements are aligned by DoD GIG Ops, OCO, and DCO.

Cyber Component. To accommodate the complexity and to provide for cyber as a warfighting domain, combatant commanders must establish a standing joint force cyber component command achieve cross-domain synergy. The advantages are greater unity of effort, a less encumbered component staff that can focus on achieving cross-domain synergy, and a component commander that is accountable to the CCDR for the cyber domain. The disadvantage is both time and resources. This approach is resource intensive and requires time to identify and build the right capabilities. This generates risk in both the operational force as implementing a structure short of a component under current doctrine limits effectiveness and in the force management in terms of resources in a constrained environment. Likewise, implementing this fully mitigates the institutional risk and the future challenges risk.[55]

Expand Interagency Capacity and Authorities. Given the complexity of the cyber domain and the demands of cross-domain synergy, CCDRs have an increased necessity for greater interagency collaboration. This demand will increase as the cyber domain increasingly evolves driven by new technology. Greater interagency collaboration and capability enables CCDRs to understand their operating environment with a great range of capabilities and perspectives. This affords establishing preconditions required for cross-domain synergy. Failing to accomplish this limits combatant commanders in their ability and scope to understand cyberspace in

peacetime conditions and set preconditions with existing authorities. The CCDR accepts greater risk in the near term because current organization employs specific processes and authorities that are not scaled to meet demand.

Conclusion

> The five domains are interdependent so JFCs must think of cyberspace as another operational domain where significant military advantage can be created and capitalized on in order to achieve U.S. national policy and military objectives.[56]

As the President has directed and reinforced through military guidance, the cyber domain presents a challenge for the combatant commander. As the focal point for the integration of military power, they are already operating in the contested domain of cyber without the benefit of cross-domain synergy. If it is a national imperative to mitigate operational and future challenges risk, CCDRs require the resources, authorities, and doctrine to accomplish their missions and responsibilities in the short term.

This requirement drives for clarity in emerging cyber doctrine and concepts. Combatant commanders seeking cross-domain synergy requires common understanding. As with the other warfighting domains, joint doctrine provides a comprehensive and established framework that enhances this appreciation. The JOAC frames the future operating environment for a CCDR. Adhering to this framework provides the ability to transcend narrowly focused application to gain cyber superiority as an end to itself but as a part of a larger construct to achieve national security objectives. Combatant commanders will remain the focal point of all operations and require the cross-domain synergy that the cyber domain underpins.

Endnotes

[1] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1-0 (Washington, DC: U.S. Joint Chiefs of Staff, March 20, 2009), I-6.

[2] Major General Michael J. Basla, "The Cyber Domain: How Is It Changing the Warfighter?," *Royal Uniformed Service Institute Defence Systems*, (June 2009): 46.

[3] U.S. Joint Chiefs of Staff, Doctrine *for the Armed Forces of the United States*, I-6.

[4] There are emerging frameworks for norms in cyberspace but no binding treaties or international governing bodies dealing with international security.

[5] While not the subject of this paper, the role and the relationship that the U.S. Military had in the Arab Spring requires detailed analysis to gauge the understanding of shaping and supporting diplomatic efforts.

[6] Barack Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 1.

[7] George W. Bush, National Security Presidential Directive 54 (Washington DC: The White House, January 2008).

[8] U.S. Government Accountability Office, *Cyber Accountability GAO-09-432T* (Washington, DC: U.S. Government Accountability Office, March 10, 2009), 1.

[9] Barack Obama, *Sustaining U.S. Global Leadership; Priorities for 21st Century* (Washington DC: The White House, January 2012).

[10] U.S. Joint Chiefs of Staff, *National Military Strategy* (Washington DC: U.S. Joint Chiefs of Staff, February 8, 2011), 8.

[11] Ibid., 10.

[12] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept* (Washington DC: Joint Chiefs of Staff, November 22, 2011).

[13] Ibid., page i. Actions and capabilities designed to limit an opposing force's freedom of action within an operating area.

[14] Ibid.

[15] Ibid.

[16] U.S. Joint Chiefs of Staff, *Joint Concept for Cyberspace* (Washington DC: Joint Chiefs of Staff, October 25, 2011), 2.

[17] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept*, i.

[18] Department of the Navy, *The U.S. Navy's Vision for Information Dominance* (Washington DC: Department of the Navy, May 2010).

[19] Department of the Air Force, "Career Field Descriptions," http://www.airforce.com/careers/detail/cyberspace-operation-officer/# (accessed February 15, 2012).

[20] U.S. Government Accountability Office, *Defense Department Cyber Efforts* GAO-11-75 (Washington, DC: U.S. Government Accountability Office, 13 July 2011), 1.

[21] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, I-11.

[22] Ibid., I-8.

[23] Ibid., I-9.

[24] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, 11 August 2011), I-6.

[25] This has been a source of tension for functional combatant commanders as they have sought to command operations in the geographical combatant commands but is beyond the scope of this paper.

[26] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, XIV.

[27] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, I-14.

[28] Ibid., I-2.

[29] Ibid., Appendix B-1.

[30] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington DC: Joint Chiefs of Staff, August 11, 2011), II-1.

[31] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Appendix B-2.

[32] U.S. Joint Chiefs of Staff, *Joint Operations*, I-7.

[33] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 83.

[34] Ibid., 246.

[35] U.S. Joint Chiefs of Staff, *Joint Concept for Operating in Cyberspace* (Washington DC: Joint Chiefs of Staff, October 25, 2011), 4.

[36] U.S. Joint Chiefs of Staff, *Joint Operations*, II-3.

[37] Ibid., III-1.

[38] Ibid., xvi.

[39] Ibid., II-4.

[40] Ibid., II-5.

[41] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept*, 15.

[42] U.S. Joint Chiefs of Staff, *Joint Operations Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), III-2.

[43] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept*, 7.

[44] U.S. Joint Forces Command, *Joint Operating Environment 2010* (Norfolk: U.S. Joint Forces Command, March 15, 2010).

[45] U.S. Joint Chiefs of Staff, *Joint Concept for Cyberspace* (Washington DC: Joint Chiefs of Staff, October 25, 2011), 25.

[46] U.S. Joint Chiefs of Staff, *Joint Operations*, III-10.

[47] U.S. Joint Chiefs of Staff, *Joint Operational Access Concept*, 4.

[48] Ibid., 16.

[49] Ibid., 17.

[50] Ibid., 16.

[51] U.S. Joint Chiefs of Staff, *Joint Operations*, III-4. A global campaign is one that requires the accomplishment of military strategic objectives within multiple theaters that extend beyond the AOR of a single GCC.

[52] Ibid., III-2.

[53] Ibid., III-3.

[54] Author's personal experience at U.S. European Command Austere Challenge. The 11 Mission Sets developed by Major General “Punch” Moulton, U.S. European Command J3. He established these over the course of meetings from August 2010 to May, 2011. The command used them in Exercise Austere Challenge.

[55] Robert M. Gates, *Department of Defense Quadrennial Defense Review* (Washington DC: U.S. Department of Defense, February 2010).

[56] U.S. Joint Chiefs of Staff, *Joint Concept for Cyberspace*, 1.